

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re the Patent Application of)

Takuya WADA et al.)

Serial No. To be assigned)

Filed: August 8, 2000)

For: RANDOM NUMBER GENERATION)
APPARATUS AND RANDOM NUMBER)
GENERATION METHOD)

ATT: APPLICATION BRANCH

JC598 U.S. PTO

09/634841

CLAIM TO PRIORITY UNDER 35 U.S.C. 119Assistant Commissioner for Patents
Washington, D.C. 20231

Sir:

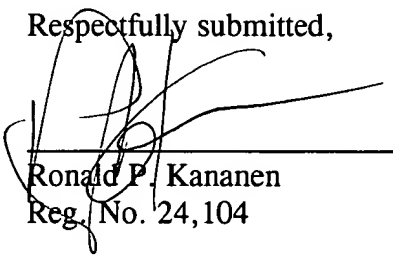
The benefit of the filing date of the following prior application filed in the following foreign country is hereby requested and the right of priority provided under 35 U.S.C. 119 is hereby claimed:

Japanese Patent Appl. No. P11-226555. filed August 10, 1999

In support of this claim, filed herewith is a certified copy of said original foreign application.

Respectfully submitted,

Dated: August 8, 2000


Ronald P. Kananen
Reg. No. 24,104

RADER, FISHMAN & GRAUER P.L.L.C.
1233 20TH Street, NW
Suite 501
Washington, DC 20036
202-955-3750-Phone
202-955-3751 - Fax

Customer No. 23353

S 00p 0947 #5

日 本 国 特 許 庁
PATENT OFFICE
JAPANESE GOVERNMENT



別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出 願 年 月 日
Date of Application:

1 9 9 9 年 8 月 1 0 日

出 願 番 号
Application Number:

平成 1 1 年特許願第 2 2 6 5 5 5 号

出 願 人
Applicant (s):

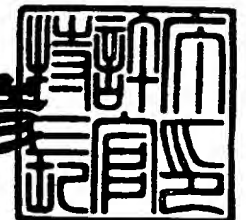
ソニー株式会社

CERTIFIED COPY OF
PRIORITY DOCUMENT

2 0 0 0 年 6 月 2 9 日

特 許 庁 長 官
Commissioner,
Patent Office

近 藤 隆 彦



出証番号 出証特 2 0 0 0 - 3 0 4 9 9 5 1

【書類名】 特許願

【整理番号】 9900368902

【提出日】 平成11年 8月10日

【あて先】 特許庁長官殿

【国際特許分類】 G06F 7/58
G06T 7/00

【発明者】

 【住所又は居所】 東京都品川区北品川 6 丁目 7 番 3 5 号 ソニー株式会社
 内

 【氏名】 和田 拓也

【発明者】

 【住所又は居所】 東京都品川区北品川 6 丁目 7 番 3 5 号 ソニー株式会社
 内

 【氏名】 塚村 善弘

【特許出願人】

 【識別番号】 000002185

 【氏名又は名称】 ソニー株式会社

 【代表者】 出井 伸之

【代理人】

 【識別番号】 100067736

 【弁理士】

 【氏名又は名称】 小池 晃

【選任した代理人】

 【識別番号】 100086335

 【弁理士】

 【氏名又は名称】 田村 榮一

【選任した代理人】

 【識別番号】 100096677

 【弁理士】

【氏名又は名称】 伊賀 誠司

【手数料の表示】

【予納台帳番号】 019530

【納付金額】 21,000円

【提出物件の目録】

【物件名】 明細書 1

【物件名】 図面 1

【物件名】 要約書 1

【包括委任状番号】 9707387

【プルーフの要否】 要

【書類名】 明細書

【発明の名称】 乱数発生装置及び乱数発生方法

【特許請求の範囲】

【請求項 1】 撮像手段と、

上記撮像手段が出力した撮像信号をデジタル画像に変換するデジタル画像変換手段と、

上記デジタル画像が画素値とされて記憶される記憶手段と、

上記記憶手段に記憶された上記撮像手段が被写体がない状態において出力した上記撮像信号の上記デジタル画像内の複数の画素の画素値からデジタルデータを抽出して、上記複数の画素に対応される上記デジタルデータから乱数を発生させる乱数発生手段と

を備えることを特徴とする乱数発生装置。

【請求項 2】 上記画素値は、2 ビット以上により表現されており、

上記乱数発生手段は、上記画素値を表現するビット列の最下位ビットの 2 値データを上記デジタルデータとして抽出して、上記複数の画素に対応される上記 2 値データから乱数を発生させること

を特徴とする請求項 1 記載の乱数発生装置。

【請求項 3】 上記デジタル画像は、上記画素値が 1 ビットの 2 値データとして表現される 2 値化画像であり、

上記乱数発生手段は、上記 2 値データを上記デジタルデータとして抽出して、上記複数の画素に対応される上記 2 値データから乱数を発生させること

を特徴とする請求項 1 記載の乱数発生装置。

【請求項 4】 上記乱数発生手段は、上記デジタル画像内における所定領域を構成する複数の画素の画素値から上記デジタルデータを抽出すること

を特徴とする請求項 1 記載の乱数発生装置。

【請求項 5】 上記乱数発生手段は、上記デジタルデータを、上記デジタル画像内の任意位置の上記複数の画素の画素値から抽出すること

を特徴とする請求項 1 記載の乱数発生装置。

【請求項 6】 上記乱数に基づいて暗号化鍵を生成し、又は上記乱数から得た控えデータに基づいて暗号化鍵を生成する暗号化部に備えられること

を特徴とする請求項 1 記載の乱数発生装置。

【請求項 7】 上記暗号化部は、2つの素数に基づいて上記暗号化鍵を生成する RSA 暗号方式が採用されており、上記乱数発生手段が発生させた上記乱数をもとに上記 2つの素数を生成し、当該 2つの素数を使用して上記暗号化鍵を生成すること

を特徴とする請求項 6 記載の乱数発生装置。

【請求項 8】 上記暗号化鍵が保管される保管手段を備えていること

を特徴とする請求項 6 記載の乱数発生装置。

【請求項 9】 上記暗号化部を有して、上記記憶手段に記憶された上記撮像手段が撮像した被写体に対応される上記デジタル画像に基づいて個人を特定する個人照合装置に備えられ、

上記個人照合装置は、所望の個人を特定したとき、上記暗号化部により上記暗号化鍵により平文の暗号化を行うこと

を特徴とする請求項 6 記載の乱数発生装置。

【請求項 10】 上記被写体は生体情報をなす指紋であること

を特徴とする請求項 9 記載の乱数発生装置。

【請求項 11】 被写体がない状態において撮像手段から出力された撮像信号をデジタル画像に変換し、

上記デジタル画像内の複数の画素の画素値からデジタルデータを抽出し、
上記複数の画素に対応されるデジタルデータから乱数を発生させること
を特徴とする乱数発生方法。

【請求項 12】 上記画素値は、2ビット以上により表現されており、
上記画素値を表現するビット列の最下位ビットの 2 値データを上記デジタルデータとして抽出して、上記複数の画素に対応される上記 2 値データから乱数を発生させること

を特徴とする請求項 11 記載の乱数発生方法。

【請求項 1 3】 上記デジタル画像は、上記画素値が 1 ビットの 2 値データとして表現される 2 値化画像であり、

上記 2 値データを上記デジタルデータとして抽出して、上記複数の画素に対応される上記 2 値データから乱数を発生させることを特徴とする請求項 1 1 記載の乱数発生方法。

【請求項 1 4】 上記デジタル画像内における所定領域を構成する複数の画素の画素値から上記デジタルデータを抽出することを特徴とする請求項 1 1 記載の乱数発生方法。

【請求項 1 5】 上記デジタルデータを、上記デジタル画像内の任意位置の上記複数の画素の画素値から抽出することを特徴とする請求項 1 1 記載の乱数発生方法。

【請求項 1 6】 上記乱数に基づいて暗号化鍵を生成し、又は上記乱数から得た控えデータに基づいて暗号化鍵を生成する暗号化方法において用いられることを特徴とする請求項 1 1 記載の乱数発生方法。

【請求項 1 7】 上記暗号化方法として、2 つの素数に基づいて上記暗号化鍵を生成する R S A 暗号方式が採用されており、上記乱数をもとに上記 2 つの素数を生成し、当該 2 つの素数を使用して上記暗号化鍵を生成するものを用いることを特徴とする請求項 1 6 記載の乱数発生方法。

【請求項 1 8】 上記暗号化方法では、当該暗号化方法により暗号化を行う装置内に上記暗号化鍵が保管されることを特徴とする請求項 1 6 記載の乱数発生方法。

【請求項 1 9】 上記暗号化方法では、上記撮像手段が撮像した被写体に対応される上記デジタル画像に基づいて所望の個人が特定されたとき、上記暗号化鍵により平文が暗号化されることを特徴とする請求項 1 6 記載の乱数発生方法。

【請求項 2 0】 上記被写体は生体情報をなす指紋であることを特徴とする請求項 1 9 記載の乱数発生方法。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】

本発明は、乱数を発生させる乱数発生装置、及び乱数発生方法に関する。

【0002】

【従来の技術】

従来、コンピュータ上で乱数を生成する方法には、線形合同法若しくは乗算合同法又はシフトレジスタ若しくはデータ暗号化規格の一つであるDES (Data Encryption Standard) によるもの等があった。

【0003】

【発明が解決しようとする課題】

ところで、上述した方法で生成された乱数は、必然的に規則性をもち、周期性が短いという欠点があった。このような乱数を、暗号化鍵や暗号化鍵を生成するためのシードの生成のため、又はメッセージの暗号化のために使用するのとは適切とはいえない。

【0004】

そこで、本発明は、上述の実情に鑑みてなされたものであり、周期性の長い乱数を発生させる乱数発生装置及び乱数発生方法を提供することを目的としている。

【0005】

【課題を解決するための手段】

本発明に係る乱数発生装置は、上述の課題を解決するために、撮像手段と、撮像手段から出力された撮像信号をデジタル画像に変換するデジタル画像変換手段と、デジタル画像が画素値とされて記憶される記憶手段と、記憶手段に記憶された撮像手段が被写体がない状態において出力した撮像信号のデジタル画像内の複数の画素の画素値からデジタルデータを抽出して、複数の画素に対応されるデジタルデータから乱数を発生させる乱数発生手段とを備える。

【0006】

このような構成を有する乱数発生装置は、撮像手段から出力された撮像信号を

デジタル画像変換手段によりデジタル画像に変換し、このデジタル画像の画素値を記憶手段に記憶する。そして、乱数生成装置は、記憶手段に記憶された撮像手段が被写体がない状態において出力した撮像信号のデジタル画像内の複数の画素の画素値からデジタルデータを抽出して、複数の画素に対応されるデジタルデータから乱数を乱数発生手段により発生させる。

【 0 0 0 7 】

これにより、被写体がない状態において得たデジタル画像の各画素の画素値に規則性がないことから、乱数発生装置により発生される乱数は、周期性の長いものとなる。

【 0 0 0 8 】

また、本発明に係る乱数発生方法は、上述した課題を解決するために、被写体がない状態において撮像手段から出力された撮像信号をデジタル画像に変換し、デジタル画像内の複数の画素の画素値からデジタルデータを抽出し、複数の画素に対応されるデジタルデータから乱数を発生させる。

【 0 0 0 9 】

これにより、被写体がない状態において得たデジタル画像の各画素の画素値に規則性がないことから、乱数発生方法により発生される乱数は、周期性の長いものとなる。

【 0 0 1 0 】

【発明の実施の形態】

以下、本発明の実施の形態について図面を用いて詳しく説明する。この実施の形態は、図 1 に示すように、A/D変換部 1、乱数発生部 3 と暗号化手段 4 とを有する暗号化部 2、CPU 5、メモリ 6、I/F部 7、及び指紋照合部 8 を備える指紋照合装置についてのものである。ここで、A/D変換部 1、乱数発生部 3、及びメモリ 6 からなる構成は、本発明に係る乱数生成装置の構成の一例をなす。

【 0 0 1 1 】

指紋照合装置は、撮像部 10 により取得した指紋画像に基づいて所望の個人を特定する個人照合装置をなすように構成されている。この指紋照合装置は、生体

情報である指紋画像に基づいて所望の個人を特定することができたときに、乱数発生部 3 において発生された乱数をもとに暗号化鍵を生成して、平文を暗号化するように構成されている。

【0 0 1 2】

撮像部 1 0 は、生体情報をなす指紋を撮像するように構成されている。具体的には、撮像部 1 0 は、図 2 に示すように、光源 1 1、プリズム 1 2、及び撮像手段 1 3 を備えている。

【0 0 1 3】

プリズム 1 2 は、断面三角形状をなしており、第 1 の面 1 2 a から光源 1 1 からの光が入射されて、第 2 の面 1 2 b 上に置かれた被写体において反射された光を第 3 の面 1 2 c から出射する。ここで、被写体は、個人を特定するための指 1 0 0 の指紋である。撮像手段 1 3 は、第 3 の面 1 2 c から出射された光が受光される位置に配置されている。撮像手段 1 3 は、例えば、CCD (Charge-Coupled Device) カメラである。

【0 0 1 4】

このような構成からなる撮像部 1 0 において、プリズム 1 2 の第 2 の面 1 2 b に指 1 0 0 が載置された場合、光源 1 1 から出射された光が第 1 の面 1 2 a から入射されて、プリズム 1 2 の第 2 の面 1 2 b 上の指 1 0 0 の指紋の隆起部で乱反射され、又は谷部分では全反射される。これら反射光は、第 3 の面 1 2 c から出射されて撮像手段 1 3 で結像される。これにより、撮像手段 1 3 では、指 1 0 0 の隆起部分が暗に部分として、また谷部分が明るい部分として撮像される。撮像手段 1 3 は、撮像情報として撮像信号を出力する。

【0 0 1 5】

撮像部 1 0 から出力された撮像信号は、適当な時間間隔で標本化され、A/D 変換部 1 において、例えば 256×128 の大きさのデジタル画像に変換される。本実施の形態では、A/D 変換部 1 は、8 ビット変換を行うように構成されており、これにより、画像を構成する各画素の画素値は、0 から 255 までの 256 階調により表現されるデジタルデータとされる。この A/D 変換部 1 において得られたのデジタル画像は、メモリ 6 上に記憶される。以下、このように 8 ビッ

ト等の多ビットにより画素値が表現されるデジタル画像をグレースケール画像という。

【0016】

画像処理部 20 は、グレースケール画像に基づいて、2 値化された画像（以下、2 値化画像という。）を生成する。例えば、画像処理部 20 は、グレースケール画像を適当なタイミングで取り込み、適当な 2 値化の方法により、8 ビットの各画素の画素値が” 0 ” 又は” 1 ” の値に変換された 2 値化画像を生成する。2 値化の方法には、画像全体の画素値の平均と各画素の画素値を比べる、または着目している画素の画素値と、当該着目している画素から所定範囲内に存在する複数の画素の画素値の平均との大小を比べる（移動平均法）といった方法がある。例えば、撮像部 10 において撮像された指紋画像は、移動平均法により 2 値化された場合、図 3 に示すような 2 値化画像として得られる。図 3 において、黒い部分は指紋の隆起部を表し、白い部分は谷部を表す。

【0017】

このように生成された 2 値化画像はこの後、細線化等の前処理がなされ、そして、登録、照合等の処理がなされる。なお、上述した移動平均法によるグレースケール画像からの 2 値化画像の取得については、後で詳しく説明する。

【0018】

指紋照合部 8 は、2 値化画像を照合する。例えば、指紋照合部 8 は、指紋情報に関して予め取得している登録画像情報と、撮像部 10 により撮像した得た指紋の 2 値化画像とを照合する。指紋照合装置は、この指紋照合部 8 における照合結果に基づいて、所望の個人を特定する。

【0019】

なお、CPU 5 は、指紋照合装置を構成する各部を制御する制御手段である。

【0020】

以上のように、指紋照合装置は、撮像部 10 により撮像して得たデジタル画像から指紋を照合して、所望の個人の特定を行う。そして、指紋照合装置は、このような指紋の照合処理により個人が特定されたときに、秘密鍵を用いて平分の暗号化を行う。この秘密鍵による暗号化は、乱数発生部 2 において発生させる乱数

をもとに取得した素数に基づいて行われる。

【 0 0 2 1 】

次に、暗号化部 2 が乱数発生部 3 により乱数を発生させ、暗号化手段 2 によりその乱数をもとに行う暗号化鍵による暗号化について説明する。なお、乱数発生部 3 は、上述したグレイスケール画像又は 2 値化画像から乱数を発生させるように構成されているが、ここでは、グレイスケール画像に基づいて乱数を発生させる場合を例に挙げて説明する。

【 0 0 2 2 】

撮像部 1 0 において、プリズム 1 2 上に指を置かずに画像の取り込み処理を実行すると、撮像手段 1 3 から出力される撮像信号にはノイズが重畳される。これにより、A/D 変換部 1 においてデジタル変換して得たグレイスケール画像の最下位ビットは不規則な " 0 " 又は " 1 " の値を示すことになる。例えば、2 値化画像についても同様に不規則な値を示す。よって、グレイスケール画像において、適当な場所をスタートアドレスとした適当な長さのビットシーケンスにより、任意の長さの " 0 " 及び " 1 " からなる乱数を得ることができる。例えば、グレイスケール画像において、最下位ビットが " 0 " のときを黒、" 1 " のときを白として場合、図 4 に示すような 2 値画像が得られる。この図 4 に示されるように、グレイスケール画像の最下位ビットには規則性がないことがわかる。

【 0 0 2 3 】

暗号化部 2 は、このように乱数発生部 3 において得られる乱数をもとに暗号化鍵又は暗号化鍵の元になるシード（控えデータ）を生成し、暗号化手段 4 において暗号化している。

【 0 0 2 4 】

一般に、暗号化鍵を生成するには、乱数をそのまま鍵とする場合と乱数をもとにして鍵をつくる場合とがある。前者の例には、DES (Data Encryption Standard)、後者の例には非常に大きな数を素因数分解が困難であることを利用した RSA 暗号方式がある。なお、RSA 暗号方式は、MIT の Rivest, Shamit 及び Adleman によって発明された暗号方式である。本実施の形態では、乱数発生部 3 は、RSA 暗号方式が採用されて、暗号化鍵を生成しており、この場合について説

明する。

【0025】

また、RSA暗号方式では、384、512又は1024ビットの鍵を生成して暗号化しているが、以下では、512ビットの鍵を生成する場合について説明する。RSA暗号方式の概要は以下のようになる。

【0026】

RSA暗号方式では、2つの素数 p 、 q 及び公開鍵の一つである公開鍵 E (public exponent) から、(1) 式及び (2) 式を用いてもう一つの公開鍵である公開鍵 N (modulus) と秘密鍵 D (private exponent) とを求める。

【0027】

$$N = p \times q \quad \dots (1)$$

$$D = E^{-1} \bmod \{ (p-1) \times (q-1) \} \quad \dots (2)$$

ここで、公開鍵 E と、 $(p-1)$ と $(q-1)$ との乗算値とは、互いに素とされている。このとき、メッセージ (平文) を M 、暗号化されたメッセージを C とすると (3) 式及び (4) 式のような関係が成り立つ。

【0028】

$$C = M^E \bmod N \quad \dots (3)$$

$$M = C^D \bmod N \quad \dots (4)$$

公開鍵 N は、512ビットの非常に大きな数であり素因数分解を行うことは非常に困難であることから、受け手側では、秘密鍵 D を知らない限り暗号化されたメッセージ C から元のメッセージ M を求めることはできない。また、デジタル署名を行う、すなわちメッセージ C に自分の署名を付けて受け手側に送るためには、送り手側の署名を付けたメッセージ C を自分の秘密鍵 D を用いて (4) 式に従って暗号化して、メッセージ M を送る。受け手側では、送り手の公開鍵 E 及び公開鍵 N を用いて (3) 式に従って復号化し、送り手の署名が付けられていることを確認する。

【0029】

以上がRSA暗号方式の概要である。RSA暗号方式を採用する暗号化手段4では、512ビットの鍵が必要とされるが、乱数発生部3において発生される乱

数が、そのように 5 1 2 ビットの鍵を生成するために使用されるものとなる。5 1 2 ビットの鍵の生成は、次のように乱数の生成により可能とされる。

【 0 0 3 0 】

鍵の長さが 5 1 2 ビットであることから、先ず、乱数発生部 3 において 2 5 6 ビットの乱数を 2 個発生させる。この 2 個の乱数が 2 個の素数を見つけるためのシードすなわち初期値となる。

【 0 0 3 . 1 】

上述したように、乱数を発生させる場合には、指紋照合装置は、プリズム 1 2 上に指 1 0 0 を置かずに画像の取り込み処理を実行し、A/D変換部 1 によりデジタル画像とされたグレイスケール画像を取得する。そして、指紋照合装置は、グレイスケール画像を、メモリ 6 上に、水平方向に 2 5 6 画素、垂直方向に 1 2 8 画素の大きさであって、画素値が 8 ビットにより表現されるものとして記憶する。なお、指紋照合装置は、このようなグレイスケール画像の取得と同時に画像処理部 2 0 においてこのグレイスケール画像から 2 値化画像も取得する。そして、指紋照合装置は、2 値化画像を、メモリ 6 上に、水平方向に 2 5 6 画素、垂直方向に 1 2 8 画素の大きさであって、画素値が 1 ビットにより表現されるものとして記憶する。

【 0 0 3 2 】

上述したようにグレイスケール画像における画素の画素値の最下位ビットは規則性がないことから、複数の画素についての画素値の最下位ビットを抽出することにより周期性の長い乱数を発生させることができるので、乱数発生部 3 は、グレイスケール画像におけるスタートアドレスにある画素から所定領域を構成する複数の画素の画素値の最下位ビットを抽出して、乱数を発生させる。ここで、スタートアドレスとは、最下位ビットの抽出を開始する画素の位置を示す情報である。

【 0 0 3 3 】

具体的には、次のように、スタートアドレスから水平方向に画素を走査して画素値の最下位ビットの値である” 0 ” 又は” 1 ” を抽出する。水平方向アドレスを i とし、垂直方向アドレスを j をとして、グレイスケール画像上における任意

の画素を $g(i, j)$ とする。

【0 0 3 4】

例えば、スタートアドレスを $(128, 0)$ として、画素 $g(128, 0)$ のから画素 $g(129, 255)$ までの 512 個の画素を走査することにより、最下位ビットの値を抽出し、256 ビットからなる 2 個の乱数を生成する。

【0 0 3 5】

また、画面上決められた場所ではなく、適当なスタートアドレスを決めて、乱数を生成することもできる。この場合、7 ビットにより 0 から 127 までの値が表現されることから、画素 $g(0, 0)$ の画素値 8 ビット及び画素 $g(0, 1)$ の画素値の下位 7 ビットで指定される水平アドレス i 及び垂直方向アドレス j をスタートアドレスとして画素の画素値の最下位ビットの値を抽出していき、乱数を生成する。例えば、画素 $g(0, 0)$ の画素値 8 ビットにより示される値が 100 であり、画素 $g(0, 1)$ の画素値の下位 7 ビットにより示される値が 23 である場合、画素 $g(100, 23)$ から画素値の最下位ビットを抽出していき乱数を生成する。

【0 0 3 6】

さらに、水平方向に隣り合った画素の間になんらかの相関があるときにはある特定のパターン（乱数）が生成され易くなるのでこれを考慮して画素値の最下位ビットを抽出していくこともできる。例えば、垂直方向に走査して画素値の最下位ビットを抽出する。また、垂直方向に隣り合う画素の間で排他的論理和演算を行い、1 ビットデータを抽出することもできる。または、画像の取り込みを 2 回行い 2 枚の画像の間で排他的論理和演算を行い、1 ビットデータを抽出することもできる。

【0 0 3 7】

以上のように、乱数発生部 3 は、画素の画素値の最下位ビットを抽出していくことにより、周期性の長い完全な乱数を発生させている。そして、暗号化手段 4 は、乱数生成部 3 において発生された 2 個の乱数の各々から 2 つの素数 p , q を生成し、暗号化鍵を生成する。暗号化手段 4 は、図 5 に示すように、素数生成工程、及び鍵生成工程の各工程を経て暗号化鍵を生成する。

【0038】

先ず、図5に示すように、ステップS1においてグレイスケール画像の画素値（グレイスケールデータ）の最下位ビットにより発生された乱数をもとに、暗号化手段4は、ステップS2～ステップS5の素数生成工程において素数を生成する。なお、以下の処理は、2個の乱数 p 、 q についてそれぞれなされるものである。

【0039】

ステップS2に示すように、暗号化手段4は、最上位ビット及び最下位ビットを”1”にセットする。これにより、ステップS1において発生された乱数は、長さが256ビット長とされかつ奇数とされる。

【0040】

続くステップS3において、暗号化手段4は、256以下の全ての素数で乱数を割り算し、乱数が256以下の全ての素数で割り切れるか否かを確認する。ここで、暗号化手段4は、乱数が256以下の全ての素数で割り切れない場合にはステップS4に進み、乱数が256以下の全ての素数で割り切れた場合にはステップS5に進む。

【0041】

ステップS4では、暗号化手段4は、代表的な確率的素数判定法であるRabin-Miller法を用いて、ステップS3において256以下の全ての素数でわり算のテストをした乱数が素数か否かをさらに確認する。ここで、暗号化手段4は、素数であると確認できた場合にはステップS6に進み、素数でないとされた場合にはステップS5に進む。

【0042】

ステップS3において乱数が素数で割り切れたとされた場合にも実行するステップS5では、暗号化手段4は、乱数 p （又は乱数 q ）の値から2が減算される。そして、暗号化手段4は、ステップS3に戻り、2が減じられた乱数が256以下の全ての素数で割り切れるか否かを再び確認し、上述したようなステップS3又はステップS5以降の処理を行う。

【 0 0 4 3 】

ステップ S 6 では、鍵生成の工程として、暗号化手段 4 は、2 個の素数 p 、 q に基づいて上述した (1) 式により公開鍵 N を取得して、この公開鍵 N と適当に選んだ公開鍵 E とから上述した (2) 式を満たす秘密鍵 D を求める。例えば、拡張ユークリッドアルゴリズムにより上述した (2) 式を満たす秘密鍵 D を求める。

【 0 0 4 4 】

以上のように、素数生成工程及び鍵生成工程により、乱数生成工程において生成された乱数は、最上位ビット及び最下位ビットが " 1 " にセットされることにより、長さが 2 5 6 ビット長とされかつ奇数とされる。そして、この乱数は、2 5 6 以下の全ての素数により順々に割り算され、その全ての素数で割り切れないことが確認される。2 5 6 以下の全ての素数で割り切れないことが確認された乱数は、代表的な確率的素数判定法である Rabin-Miller 法を用いて、テストをしている乱数が素数であるか否かをチェックされる。ここで、素数でないとされた場合には、テストしている乱数は、2 が減じられて、再び素数であるか否かが確認される。そして、素数であることが確認された乱数は、最後に (1) 式から計算された公開鍵 N 及び公開鍵 E から (2) 式を満たす秘密鍵 D を求めるために使用される。

【 0 0 4 5 】

以上のように、暗号化部 2 は、乱数発生部 3 により周期性の長い完全な乱数を生成し、暗号化手段 4 によりこの乱数をもとに素数を生成して、この素数を使用して暗号化鍵である秘密鍵 D を生成する。指紋照合装置は、秘密鍵 D を保管するための秘密鍵保管手段を有しており、このように生成された秘密鍵 D は、秘密鍵保管手段としても機能する例えばメモリ 6 に記憶されることにより、指紋照合装置内において保管される。

【 0 0 4 6 】

そして、暗号化部 2 により秘密鍵 D を用いてメッセージ (平文) が暗号化される。メッセージは、暗号化部 2 において次のように、デジタル署名が付されて暗号化される。

【 0 0 4 7 】

指紋照合装置は、指紋照合部 8 においてプリズム 1 2 上に指が置かれた際に得た 2 値化画像を照合して、本人であることを確認する。暗号化部 2 では、本人であることが確認されると、秘密鍵 D を使って、メッセージが暗号化される。ここで、指紋照合装置は、インターフェース (I / F) 部 6 を介して図示しないパーソナルコンピュータが接続されており、メッセージは、インターフェース (I / F) 部 6 を介してパーソナルコンピュータから送信されてきたものである。

【 0 0 4 8 】

指紋照合装置は、暗号化部 2 において暗号化したメッセージにデジタル署名を付けて、パーソナルコンピュータに送り返す。

【 0 0 4 9 】

パーソナルコンピュータでは、このようにデジタル署名を付されて暗号化されたメッセージを、所望の相手に対してネットワークを介して送信する処理を行う。

【 0 0 5 0 】

以上のように、指紋照合装置は、所望の個人を特定できたときに、暗号化鍵を使用してメッセージを暗号化して、当該暗号化したメッセージを所望の相手に送っている。

【 0 0 5 1 】

この指紋照合装置は、上述したように、プリズム 1 2 上に指 1 0 0 を置かない状態において撮像部 1 0 において取得したグレイスケール画像の最下位ビットを使用することにより、周期性の長い乱数を得ている。これにより、指紋照合装置は、そのような乱数をもとに暗号化に使用する素数を生成することにより、信頼性の高い暗号化を提供することができる。

【 0 0 5 2 】

さらに、指紋照合装置は、暗号化に使用する秘密鍵 D を秘密鍵専用の保管手段に格納し、接続されているパーソナルコンピュータ等の外部機器に秘密鍵 D を見られることなく暗号化を実行しているので、信頼性の高い暗号化を提供することができる。すなわち、秘密鍵 D を指紋照合装置内に保持して、指紋照合装置内で

全ての暗号化を実行することにより、秘密鍵Dが第三者に読まれることはなく、乱数発生から暗号化までの一連の処理を、指紋照合装置といった同一の装置内において行うことができるので、当該暗号化はセキュリティーが向上されたものとなる。

【0053】

なお、上述の実施の形態では、グレイスケール画像の画素値の最下位ビットから乱数を生成する場合について説明した。しかし、指紋照合装置は、2値化画像の各画素の画素値に基づいて乱数を発生させることもでき、次のように、2値化画像の各画素の画素値に基づいて乱数を発生させることができる。ここで、水平方向アドレスを*i*とし、垂直方向アドレスを*j*をととして、2値化画像上における任意の画素の*b* (*i*, *j*) とする。

【0054】

例えば、上述したグレイスケール画像と同様に、スタートアドレスを(128, 0)とした場合、乱数発生部3は、画素*b* (128, 0)から画素*b* (129, 255)までの各画素の画素値を抽出して、これにより256ビットからなる2個の乱数を生成する。

【0055】

また、乱数発生部3は、画面上決められた場所ではなく、適当なスタートアドレスを決めて、乱数を生成することもできる。例えば、乱数発生部3は、画素*b* (0, 0)から画素*b* (0, 7)までの画素の画素値、及び画素*b* (0, 8)から画素*b* (0, 14)までの各画素の画素値で指定される水平アドレス*i* 及び垂直方向アドレス*j* をスタートアドレスとして画素の画素値を抽出していき乱数を発生させる。例えば、画素*b* (0, 0)から画素*b* (0, 6)までの各画素の画素値により示される値が100であり、画素*b* (0, 7)から画素*b* (0, 13)までの各画素の画素値により示される値が23である場合、乱数発生部3は、画素*b* (100, 23)から画素値を抽出していき乱数を発生させる。

【0056】

また、グレイスケール画像と同様に、垂直方向に走査して画素値を抽出したり、垂直方向に隣り合う画素の間で排他的論理和演算を行い、1ビットデータを抽

出したり、画像の取り込みを 2 回行い 2 枚の画像の間で排他的論理和演算を行い、1 ビットデータを抽出したりすることもできる。乱数生成部 1 は、このような抽出により、より完全な乱数を生成することができる。

【0057】

そして、暗号化手段 4 は、このように乱数生成部 3 において 2 値化画像に基づいて生成された 2 個の乱数をもとに、上述した図 5 に示す素数生成工程、及び鍵生成工程により暗号化鍵を生成する処理を行う。すなわち、ステップ S 1 において生成された 2 値化画像の画素値（2 値化データ）に基づく乱数をもとに、以降のステップ S 2 ～ステップ S 6 における素数生成工程及び鍵生成工程を経て暗号化鍵が生成される。

【0058】

なお、画像処理部 20 は、図 6 に示すように、グレイスケール画像から 2 値化画像を生成する 2 値化画像生成部を備えている。この画像処理部 20 は、移動平均法に対応されて構成されている。本例では、中心画素の周囲の垂直方向 7 画素及び水平方向 7 画素（7 × 7 画素）の範囲の平均値を用いて行う 2 値化について説明する。

【0059】

2 値化画像生成部は、直列に 7 個接続され、256 バイトの容量を有する第 1 乃至第 7 の F I F O (first-in,first-out) 21, 22, 23, 24, 25, 26, 27 と、第 1 乃至第 7 の各 F I F O 21, 22, 23, 24, 25, 26, 27 の後段に接続され、水平方向の画素の画素値の総和を算出する水平方向総和ブロック 28, 29, 30, 31, 32, 33, 34 と、全ての水平方向総和ブロック 28, 29, 30, 31, 32, 33, 34 からの出力を加算する加算器 35 と、加算器 35 からの出力を 49 で除算する除算器 36 と、第 4 の水平方向総和ブロック 31 から出力される中心画素の画素値から除算器 36 からの出力を引き算する減算器 37 とを備えている。

【0060】

ここで、第 1 乃至第 7 の水平方向総和ブロック 28, 29, 30, 31, 32, 33, 34 では、入力データが 8 ビット幅とされている 7 個の第 1 乃至第 7 の

Dフリップフロップ 4 1, 4 2, 4 3, 4 4, 4 5, 4 6, 4 7 が直列に接続され、第 1 乃至第 7 の各 D フリップフロップ 4 1, 4 2, 4 3, 4 4, 4 5, 4 6, 4 7 からの出力を加算器 4 8 により加算している。

【0 0 6 1】

このような構成を有する 2 値化画像生成部では、第 1 の F I F O 2 1 から N 走査目のグレースケール画像の画素の画素値が出力されているときには、第 2 の F I F O 2 2 からは N - 1 走査目のグレースケール画像の画素の画素値が出力され、第 3 の F I F O 2 3 からは N - 2 走査目のグレースケール画像の画素の画素値データが出力され、このような関係とされて同様に第 4 乃至第 7 の F I F O 2 4, 2 5, 2 6, 2 7 からグレースケール画像の画素の画素値が出力される。

【0 0 6 2】

第 1 乃至第 7 の各水平方向走査ブロック 2 8, 2 9, 3 0, 3 1, 3 2, 3 3, 3 4 では、水平方向に連続する 7 個の画素の画素値の和が計算される。そして、第 1 乃至第 7 の各水平方向総和ブロック 2 8, 2 9, 3 0, 3 1, 3 2, 3 3, 3 4 からの出力は、垂直方向総和ブロックを構成する加算器 3 5 において足し合わされた後、除算器 3 6 に入力される。

【0 0 6 3】

除算器 3 6 は、加算器 3 5 からの出力である水平方向、垂直方向に加算された画素の個数 4 9 で割ることにより、2 値化のしきい値を算出する。そして、コンパレータ 3 7 により、第 4 の水平方向総和ブロック 3 1 の 2 値化のしきい値と比較され、2 値化が行われる。

【0 0 6 4】

以上のような構成を有することにより、2 値化画像生成部は、グレースケール画像から 2 値化画像を生成する。

【0 0 6 5】

乱数発生部 3 は、この 2 値化画素生成部により生成された 2 値化画像の各画素の画素値に基づいて上述したように乱数を発生させることができる。

【0 0 6 6】

また、指紋照合部 8 は、この 2 値化画像生成部により生成された 2 値化画像に

より指紋の照合処理を行っている。

【 0 0 6 7 】

【発明の効果】

本発明に係る乱数発生装置は、撮像手段から出力された撮像信号をデジタル画像に変換するデジタル画像変換手段と、デジタル画像が画素値とされて記憶される記憶手段と、記憶手段に記憶された撮像手段が被写体がない状態において出力した撮像信号のデジタル画像内の複数の画素の画素値からデジタルデータを抽出して、複数の画素に対応されるデジタルデータから乱数を発生させる乱数発生手段とを備えることにより、撮像手段から出力された撮像信号をデジタル画像変換手段によりデジタル画像に変換し、このデジタル画像の画素値を記憶手段に記憶して、この記憶手段に記憶された撮像手段が被写体がない状態において出力した撮像信号のデジタル画像内の複数の画素の画素値からデジタルデータを抽出して、複数の画素に対応されるデジタルデータから乱数を乱数発生手段により発生させることができる。

【 0 0 6 8 】

これにより、乱数発生装置は、周期性の長い乱数を生成することができる。

【 0 0 6 9 】

また、例えば、平文の暗号化の機能も有する指紋照合装置は、このような乱数を生成する乱数発生装置を備え、暗号化鍵を装置内で生成して、生成した暗号化鍵を装置内に保管することにより、安全性を向上させて暗号化を行うことができる。

【 0 0 7 0 】

また、本発明に係る乱数発生方法は、被写体がない状態において撮像手段から出力された撮像信号をデジタル画像に変換し、デジタル画像内の複数の画素の画素値からデジタルデータを抽出し、複数の画素に対応されるデジタルデータから乱数を発生させることにより、周期性の長い乱数を生成することができる。

【 0 0 7 1 】

また、例えば、平文の暗号化の機能も有する指紋照合装置は、このような乱数を生成する乱数発生方法が適用されて構成されることにより、暗号化鍵を装置内

で生成して、生成した暗号化鍵を装置内に保管することにより、安全性を向上させて暗号化を行うことができる。

【 0 0 7 2 】

【発明の効果】

【図面の簡単な説明】

【図 1】

本発明に係る暗号生成装置を暗号化部として備える指紋照合装置を示すブロック図である。

【図 2】

上述した指紋照合装置の撮像部の構成を示すブロック図である。

【図 3】

上述した指紋照合装置において得られた指紋の 2 値化画像を示す図である。

【図 4】

上述した指紋照合装置において得られた指紋のグレイスケール画像の最下位 1 ビットにより構成される画像を示す図である。

【図 5】

乱数生成工程、素数生成工程、及び鍵生成工程の各工程の処理手順を示すフローチャートである。

【図 6】

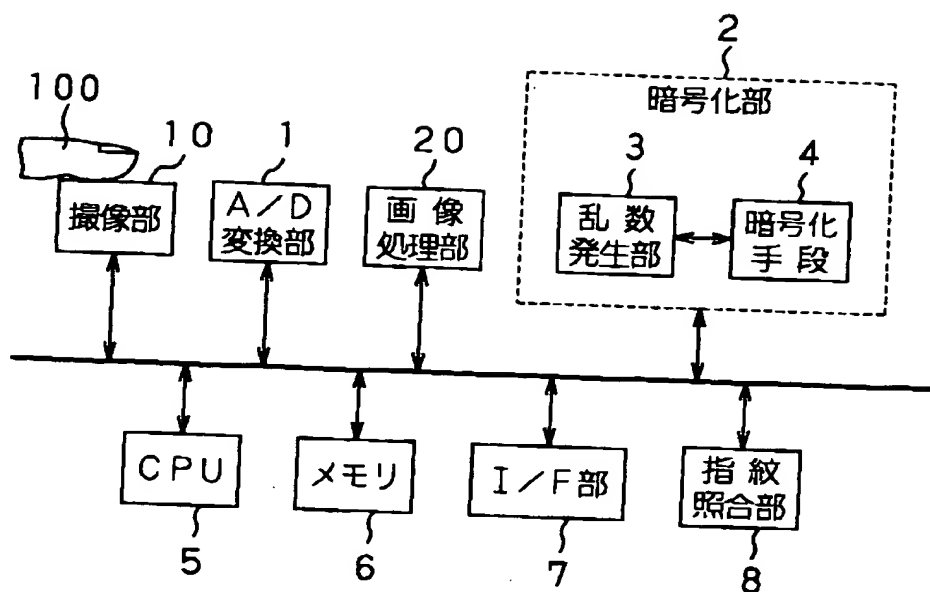
上述した指紋照合装置の画像処理部における 2 値化画像生成部を示すブロック図である。

【符号の説明】

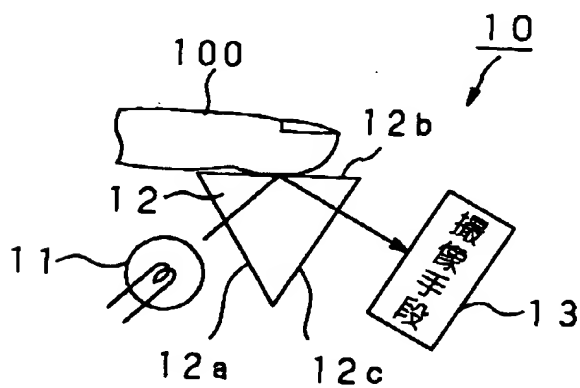
1 A/D変換部、 3 乱数発生部、 6 メモリ

【書類名】 図面

【図 1】



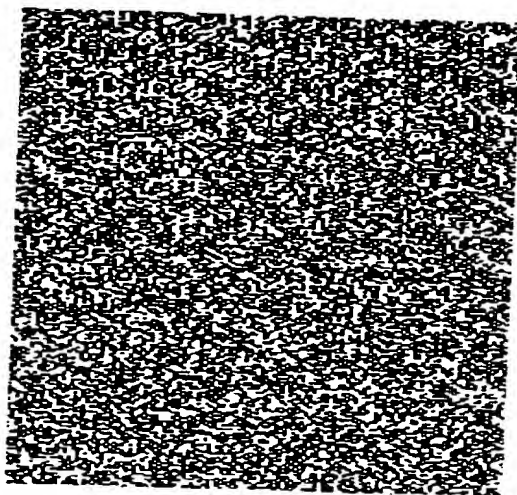
【図 2】



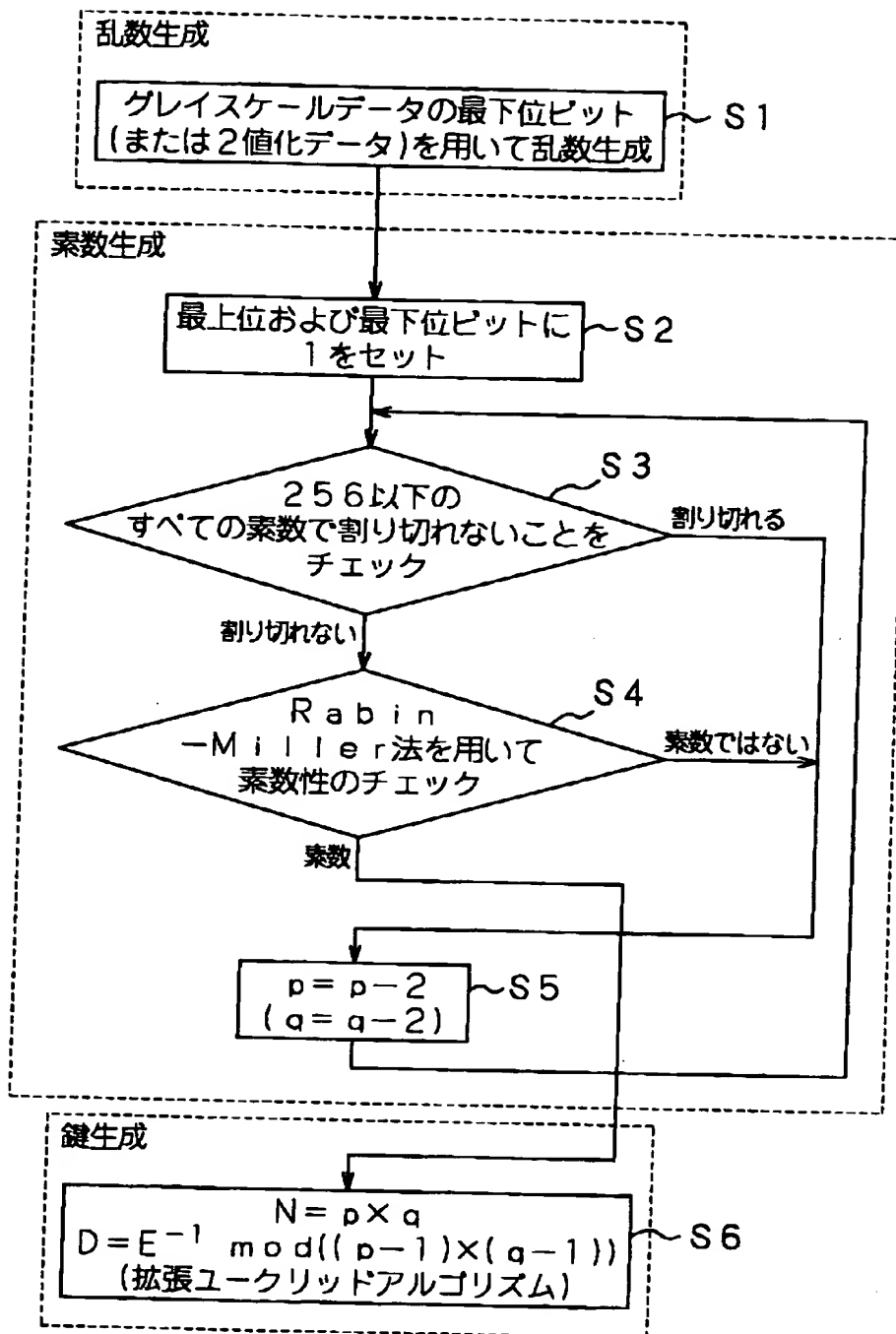
【图 3】



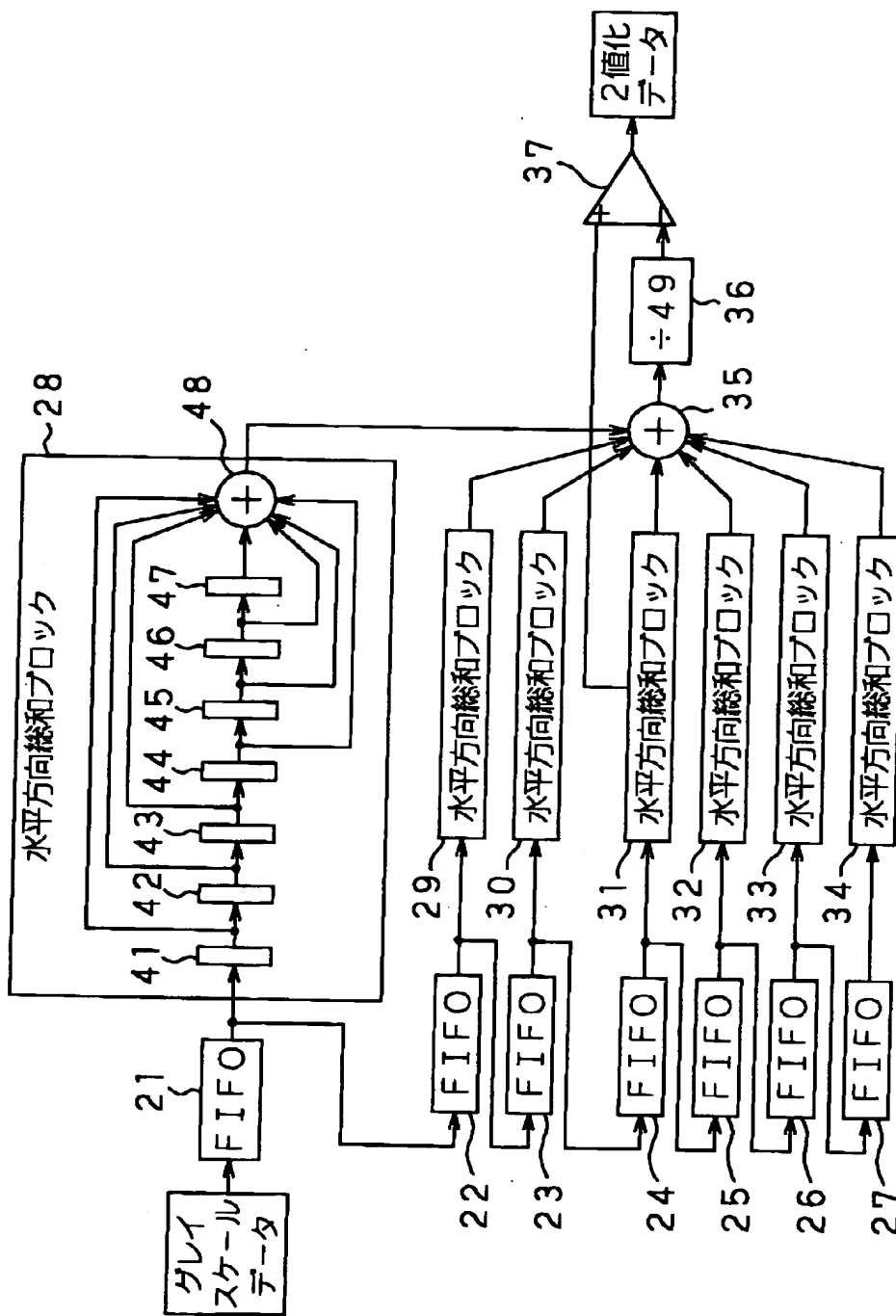
【图 4】



【図 5】



【図 6】



【書類名】 要約書

【要約】

【課題】 周期性の長い乱数を発生させること。

【解決手段】 乱数発生部分として、撮像部 1 0 から出力された撮像信号をデジタル画像に変換する A/D変換部 1 と、デジタル画像が画素値とされて記憶されるメモリ 6 と、メモリ 6 に記憶された撮像部 1 0 が被写体がない状態において出力した撮像信号のデジタル画像内の複数の画素の画素値からデジタルデータを抽出して、複数の画素に対応されるデジタルデータから乱数を発生させる乱数発生部 3 とを備える。

【選択図】 図 1

出 願 人 履 歴 情 報

識別番号 [000002185]

1. 変更年月日 1990年 8月30日
[変更理由] 新規登録
住 所 東京都品川区北品川6丁目7番35号
氏 名 ソニー株式会社